

U.S. Department of Justice

United States Attorney

Eastern District of Virginia

2100 Jamieson Avenue (703)299-3700
Alexandria, Virginia 22314

News Release

FOR IMMEDIATE RELEASE:

August 16, 2002

For Further Information:

Sam Dibbley (703-299-3822)

United States Attorney Paul J. McNulty announced today that Christopher Tresco, age 24, of Allston, Massachusetts, was sentenced to 33 months in federal prison by the Honorable T.S. Ellis, III, United States District Judge, for conspiring to violate criminal copyright laws as a member of one of the oldest and largest international software piracy rings on the Internet.

Christopher Tresco, known by his screen nickname "BigRar," was a staff member of the online software piracy group known as DrinkOrDie. DrinkOrDie was a highly organized, security-conscious, Internet software piracy group that specialized in acquiring new software, "cracking" it (i.e., stripping or circumventing its copyright protections), and releasing the software over the Internet. DrinkOrDie consisted of approximately 65 group members from more than 12 countries, including the United Kingdom, Australia, Sweden, Norway, and Finland.

DrinkOrDie concealed its illegal activities using an array of technology and security measures. Members sent e-mails via the group's private mail server using encrypted messages; members identified themselves only by screen nickname, never by their full real name, and communicated about group business only in closed, invite-only Internet Relay Chat channels; the group's Internet file transfer and storage sites (FTP sites), which contained tens of thousands of pirated software, game, movie, and music titles, were password-protected and secured by a combination of user ID and Internet Provider address authentication mechanisms. Christopher Tresco performed several important functions for the group, most of which took advantage of his employment, at the time, as a systems administrator for the Economics Department at the Massachusetts Institute of Technology (MIT) where he had unimpeded access to multiple high-speed internet connections on the university system. Tresco installed and operated a number of DrinkOrDie file storage/transfer sites on the MIT system, including DrinkOrDie's "drop site," a computer connected full-time to the internet that served as the work station and initial distribution point for all the group's release work of copyrighted material. Tresco also installed and operated on the MIT system a number of DrinkOrDie's FTP "leach" sites which contained tens of thousands of software, game, movie, and music titles for copying and downloading by DrinkOrDie members.

DrinkOrDie's organizational structure classified group members in four categories in order of importance and responsibility: Leader or co-leader, Council, Staff, and general membership. Council and Staff members generally were the most active in the group's "release"

work -- the process by which the group acquired, cracked, ripped, and distributed software over the Internet in violation of the copyright laws. Members designated as “suppliers” provided new software to the group often days or weeks before the software was commercially available. This included software manufactured not only by larger companies such as Microsoft, Adobe, Autodesk, Symantec, and Novell, but also by much smaller companies, some with as few as eight employees, whose livelihood depended on the sales revenue generated by one or two products a year. Once software was supplied, highly skilled "crackers" would permanently defeat its copyright protections, thereby allowing the software to be illegally reproduced, distributed and used by anyone obtaining a copy. The “cracked” version would then be tested, packed, and rapidly distributed over the Internet to an ever-expanding web of hundreds, if not thousands, of illegal Internet sites worldwide. “Cracked” software released by DrinkOrDie has been found on pay-for-access websites in the U.S. and abroad, including China.

Tresco is among more than 40 individuals worldwide targeted by Operation Buccaneer, a 14-month undercover investigation by the U.S. Customs Service that represents the largest international copyright piracy investigation to date by law enforcement. In addition to dismantling DrinkOrDie, Operation Buccaneer also netted members from a broad cross-section of leading online piracy groups (aka “warez groups”), including RiSC, RAZOR1911, RiSCISO, Request To Send (RTS), ShadowRealm (SRM), WomenLoveWarez (WLW), and POPZ.

To date in the Eastern District of Virginia, 13 defendants have pled guilty, ten have been sentenced. Six defendants have been formally charged in the United Kingdom as a result of Operation Buccaneer. More prosecutions are expected in the U.S. and abroad, including Australia, Finland, Sweden, and Norway.

Prosecuting these cases for the United States are Assistant U.S. Attorney Robert Wiechering; Michael DuBose, Senior Counsel, and Michael O’Leary, Trial Attorney, of the Computer Crime and Intellectual Property Section, Department of Justice. Investigation conducted by the U.S. Customs Service, including the Customs CyberSmuggling Center in Fairfax, VA, and the Washington RAIC Office in Fairfax, VA. Assistance was provided by several intellectual property trade associations, including but not limited to the Interactive Digital Software Alliance (IDSA) and the Business Software Alliance (BSA).